Pandora's Hope

User Manual

Version 2

Contents

Contents

Chapter 1:

The Family Version

1.1: The Family Version

Manufacturer: Buffalo Inc.

Model Number: WZR-HP-G300NH2 / WZR-300HP

Processor Speed: 400Mhz

Memory: 64MB

Wireless LAN Interface:

-Standards: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b

-Access Mode: Infrastructure

-Antenna: 2 x 2

-Wireless Security: WPA2, WEP

Wired LAN Interface:

-Speed: 10/100/1000 Mb/s

-Number of LAN ports: 4

-Number of WAN ports: 1

Dimensions: 6.2 x 6.5 x 1.4 in

Weight: .54 lb

Power Supply: External AC 100 – 240V, 50/60 HZ

Chapter 1:

Router Specifications

1.2: The Pro Version

Manufacturer: Buffalo Inc.

Model Number: WZR-HP-AG300H / WZR-600DHP

Processor Speed: 680Mhz

Memory: 128MB

Wireless LAN Interface:

-**Standards:** IEEE 802.11n, IEEE 802.11g, IEEE 802.11b

-**Frequency Range:** 2.4Ghz / 5Ghz

-**Access Mode:** Infrastructure

-**Antenna:** 2 x 2

-**Wireless Security:** WPA2, WEP

Wired LAN Interface:

-**Speed:** 10/100/1000 Mb/s

-**Number of LAN ports:** 4

-**Number of WAN ports:** 1

Dimensions: 6.2 x 6.5 x 1.4 in

Weight: .73 lb

Power Supply: External AC 100 – 240V, 50/60 HZ

Chapter 2:

Connecting to Pandora's Hope

2.1a: Connecting via Wireless Network – Windows & Macintosh

-On a Windows PC (XP,Vista,7)

- Select the Wireless Network icon on the task bar

- In that list of networks will be PandorasHope

- Right-click on the PandorasHope network and click connect.
- If prompted for a password, please enter the wireless security key created during the setup wizard.
  By default it is set to your ten digit telephone number.

-On Mac OSX

- Select the AirPort icon at the top

- Click on the PandorasHope network
- If prompted for a password, please enter the wireless security key created during the setup wizard.
  By default it is set to your ten digit telephone number.

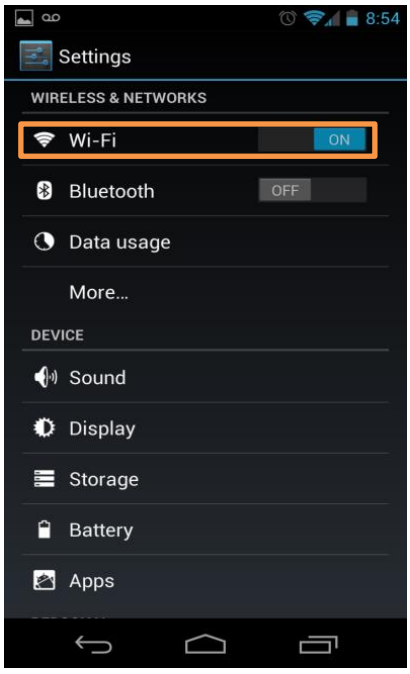
Chapter 2:

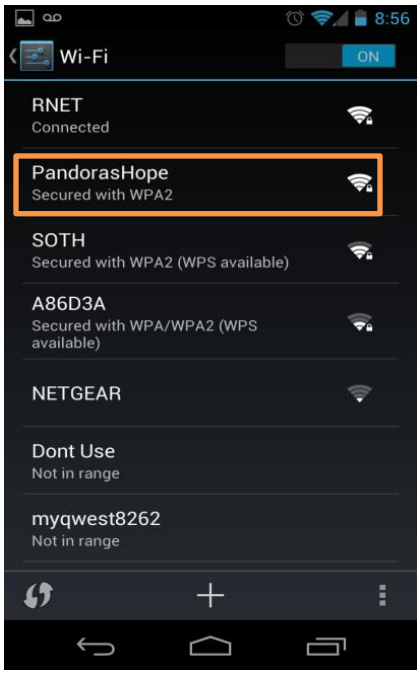
Connecting to Pandora's Hope

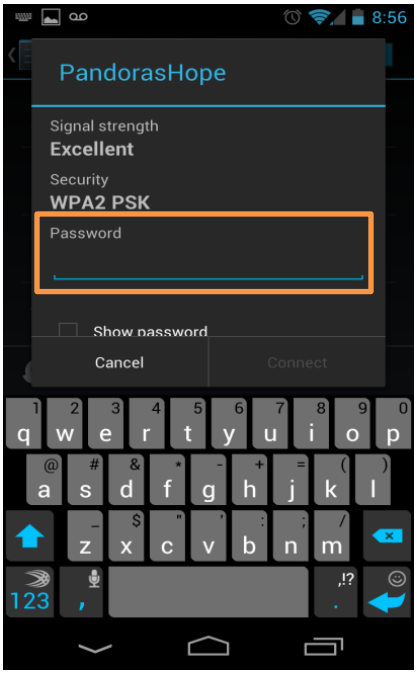
2.1b: Connecting via Wireless Network – Mobile Devices

-On Android devices

- Select the Settings icon 
- Then select the "Wireless & Networks" menu
- Select "Wi-Fi", and click on the PandorasHope network
- If prompted for a password, please enter the wireless security key created during the setup wizard.
  By default it is set to your ten digit telephone number.







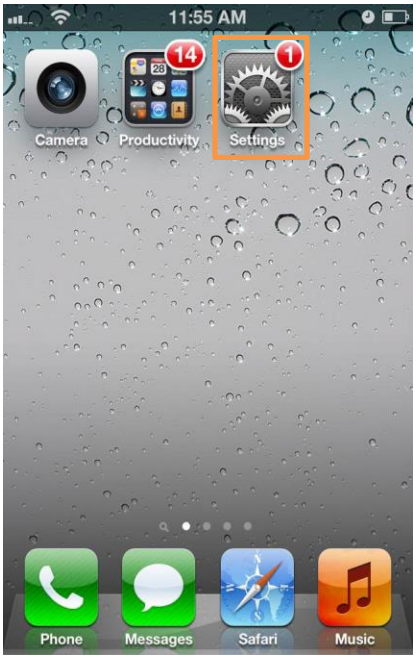
Chapter 2:

Connecting to Pandora's Hope

2.1c: Connecting via Wireless Network – Mobile Devices (Continued)

-On IOS devices (iPhone, iPod, iPad)

- Select the Settings icon 
- Select "Wi-Fi", and click on the PandorasHope network
- If prompted for a password, please enter the wireless security key created during the setup wizard.
  By default it is set to your ten digit telephone number.



Chapter 2:

Connecting to Pandora's Hope

2.2: Connecting via Ethernet

- To connect a device with an Ethernet cable, plug in one end of the ethernet cable into any of the four black ports on the back of the router. Connect the other end into the device.

Chapter 2:

The Management Interface

2.3: Accessing the Management Interface

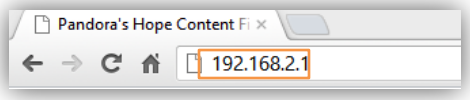
The management interface is an administrative website where the user can access important system settings and filtering tools.

To access the administrative site:

- Open an internet browser, and enter in one of these two addresses into the address bar:

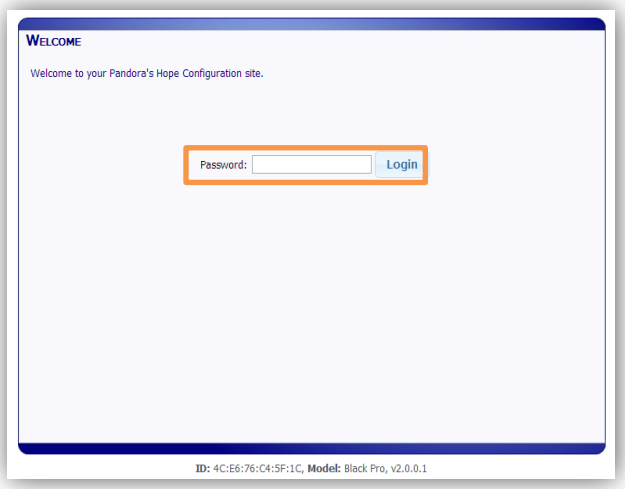
  192.168.2.1

  Local.pandorashope.com



  Alternatively, the user could navigate to **Pandorashope.com,** and then select the **My Settings** link at the top of the page.

- The user will then be directed to these pages. Click on the link to login, and enter the administrative password.



Chapter 3:

Monitoring Pandora's Hope

3.1: Filter Status

Location: View Tab > Filter Status

The filter status page displays whether the filter is enabled or disabled. It also will display any temporary bypasses that have been authorized. Please see page **4.3** for more information on temporary bypasses.

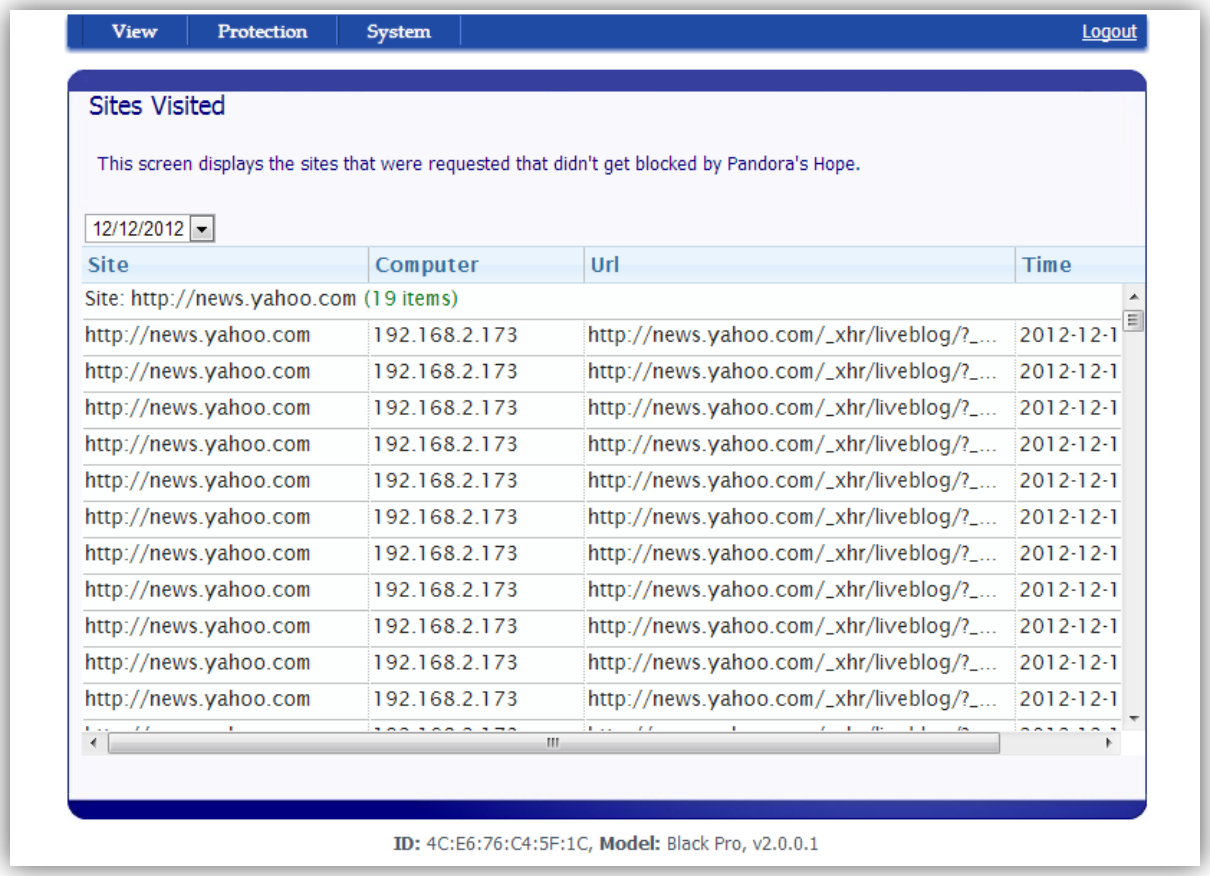
Chapter 3:

Monitoring Pandora's Hope

3.2: The Sites Visited Page

Location: View Tab > Sites Visited

The sites visited page displays all of the web traffic generated by computers and other devices. This page will provide the device's IP address, the website information, and the exact time that the page was accessed. Pandora's Hope will also archive these logs for later viewing. To select a different date, click on the drop-down menu at the top left-hand corner of the page.



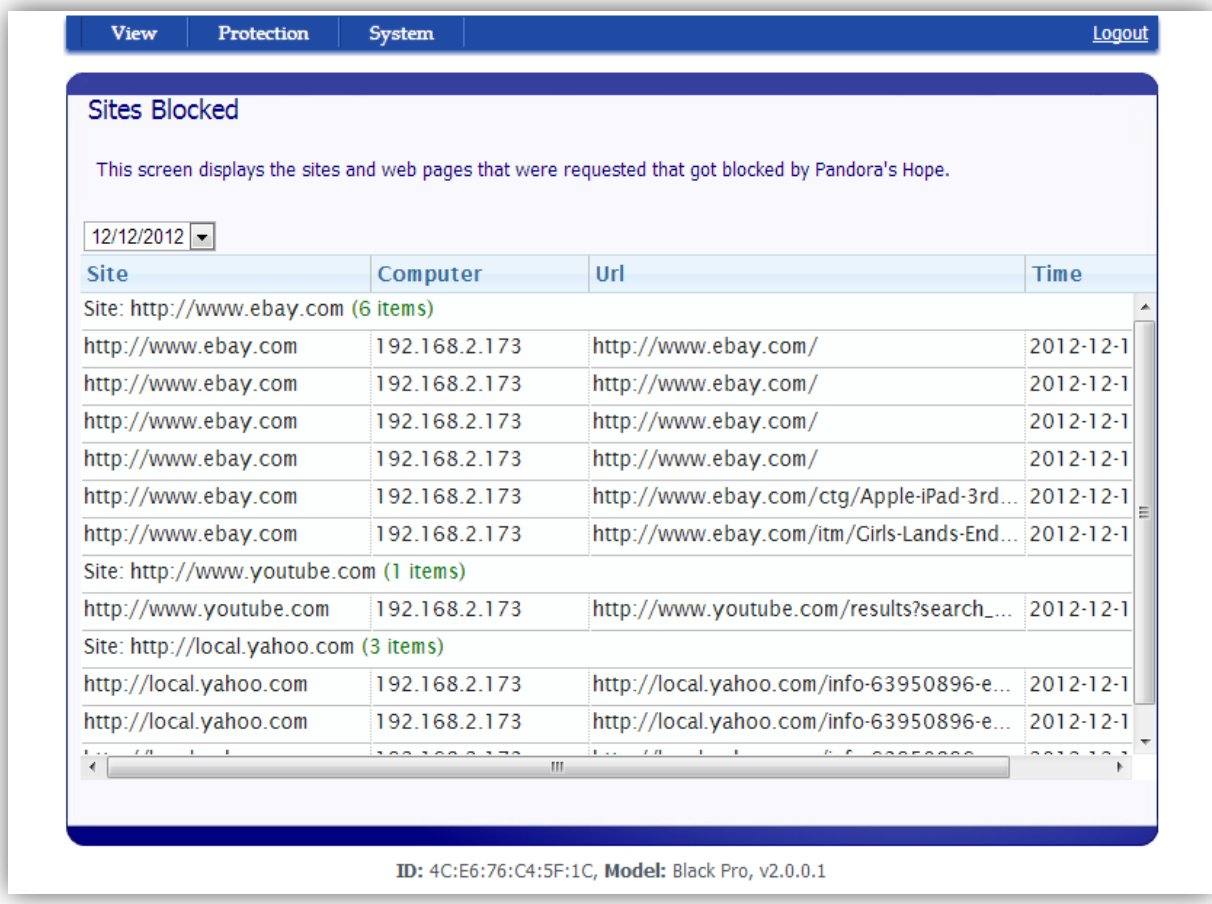
Chapter 3:

Monitoring Pandora's Hope

3.3: The Sites Blocked Page

Location: View Tab > Sites Blocked

The sites blocked page will display all of the web traffic that was blocked by Pandora's Hope. This page will provide the devices IP address, the website information, and exact time that the page was blocked. Pandora's Hope will also archive these logs for later viewing. To select a different date, click on the drop-down menu at the top left-hand corner of the page.



Chapter 3:

Monitoring Pandora's Hope

3.4: The Router Interfaces page

Location: View Tab > Interfaces

The Router Interfaces page displays interface information

Chapter 3:

Monitoring Pandora's Hope

3.4: The DHCP Clients page

Location: View Tab > DHCP Clients

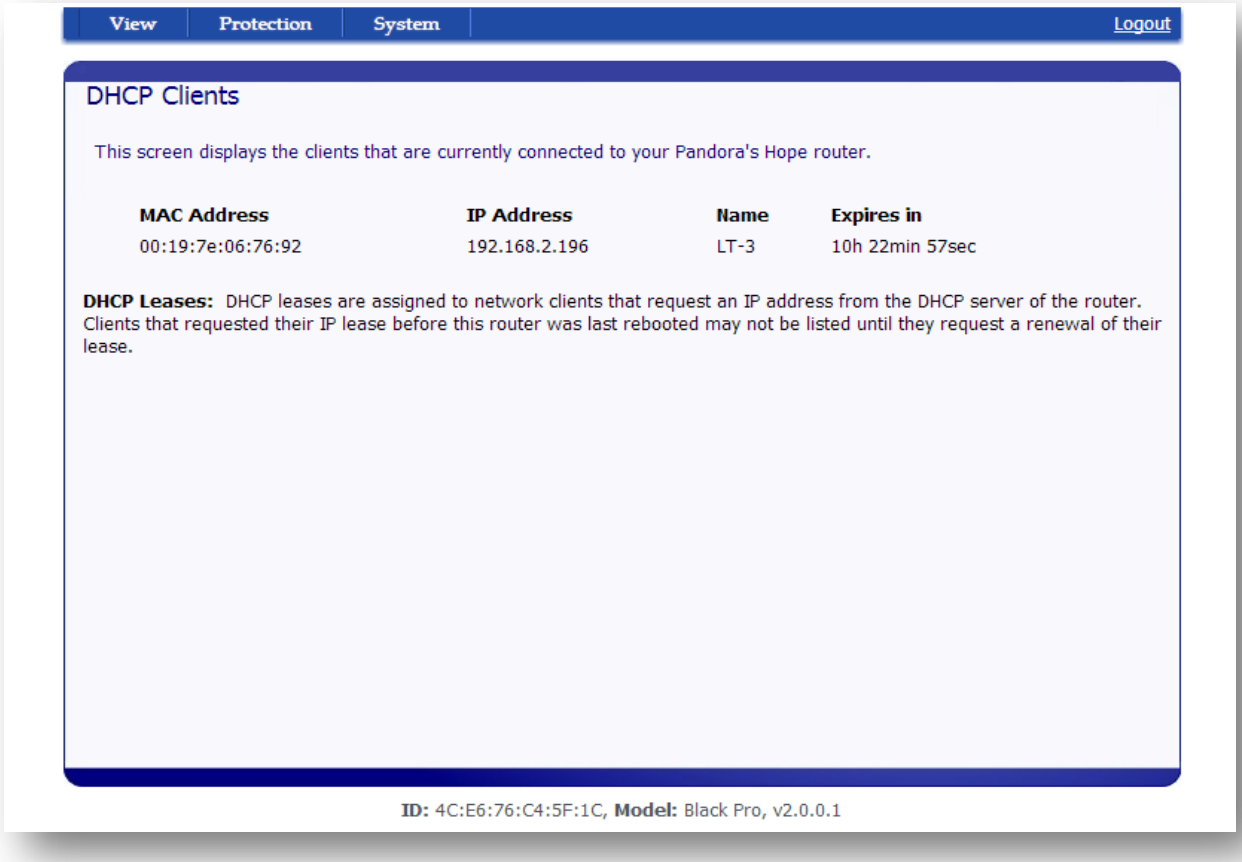
The DHCP Clients page will list all of the devices currently connected to Pandora's Hope. If a device requested its DHCP lease before Pandora's Hope was last rebooted, it will not show in this list until it requests a new lease.

Below are explanations for the various columns:

MAC Address: Media Access Control – This address serves as a unique identifier for networked devices.

IP Address: Internet Protocol Address – This is an address given to a device by the router.

Name: The name field displays the name of the device, either assigned by the user, or manufacturer of the device.



Chapter 3:

Monitoring Pandora's Hope

3.5: The Diagnostic page

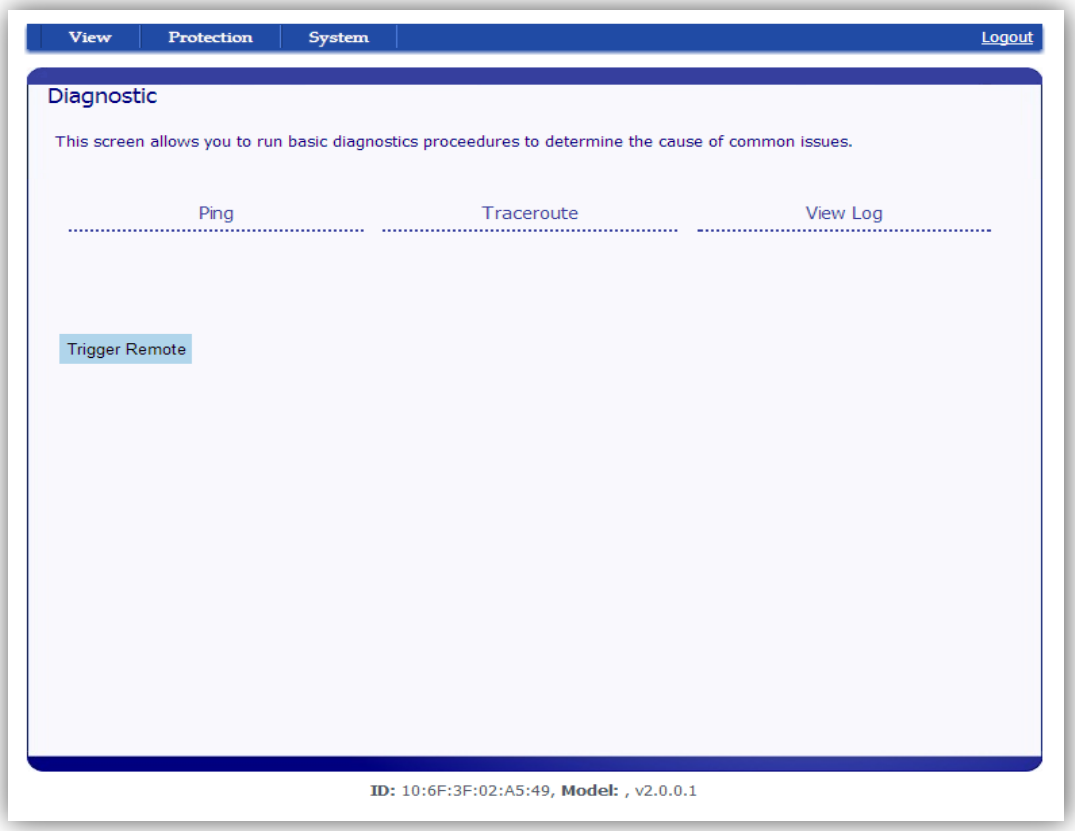
Location: View Tab > Diagnostic

Ping: This tool will attempt communicate with a specific web or IP address, and will log every "reply" received

Traceroute: This tool will attempt to communicate with a specific web or IP address, and will log every "hop" it makes along the way. To use the tool, click on the Traceroute line and enter in an address. The results will populate at the bottom of the page.

View Log: This tool will display the entire system log. This includes the output from the start-up phase, and router updates.

Trigger Remote: This option allows a user to initiate a remote connection to the Pandora's Hope technical support team. To use Trigger Remote, press the "Trigger Remote" button. If successful, you will receive a confirmation at the bottom of the page.



Chapter 4:

The Filtering Mechanism

4.1: Understanding the filter

The router works on text-based algorithms to detect inappropriate pages. Each webpage and it's URL are dynamically registered against known keywords and phrases that can trigger the blocking mechanism. The filtering system will also check the name, and URL associated with videos and images.

For Text-Based Content

The filtering system for text-based content will evaluate all of the text on a web page, and register those words against a list of keywords and phrases. The number of keywords permitted on a webpage depends on the filter strength, and the word itself. Some keywords have a greater "weight", and less of them are permitted on a webpage.

For Image-Based Content

Images are filtered based on their title and URL, evaluated against our list of keywords.

For Video-Based Content

Videos are filtered based on their title and URL, evaluated against our list of keywords

Ad-blocking

The filtering system will block advertisements, based on a list on known advertisers.

Chapter 4:

The Filtering Mechanism

4.2a: Configuring the filter: The Black list

Location: Protection Tab > Black list

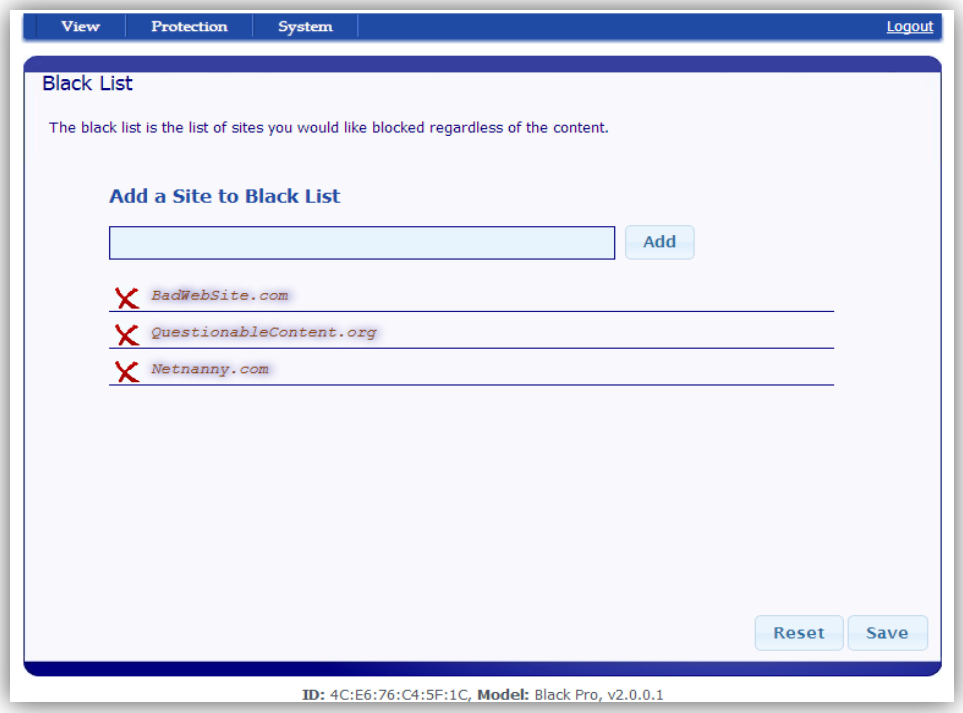
The black list is a list of websites to be blocked regardless of the content contained on them. This tool is useful for blocking websites that may not be caught by the Pandora's Hope filter, but would still be offensive to the user.

To add an entry into the black list:

- Enter in the web address into the blue area .
  (**Note**: You do not need the prefixes HTTP or WWW.)
- Click the "Add" button
- Once all of the desired addresses have been added, click "Save"
- The newly black listed websites will be blocked immediately after pressing "Save"

To remove an entry from the black list:

- Press the red "X" next to the web address
- Once all of the desired web addresses have been removed, click "Save"



Chapter 4:

The Filtering Mechanism

4.2b: Configuring the filter: The White list

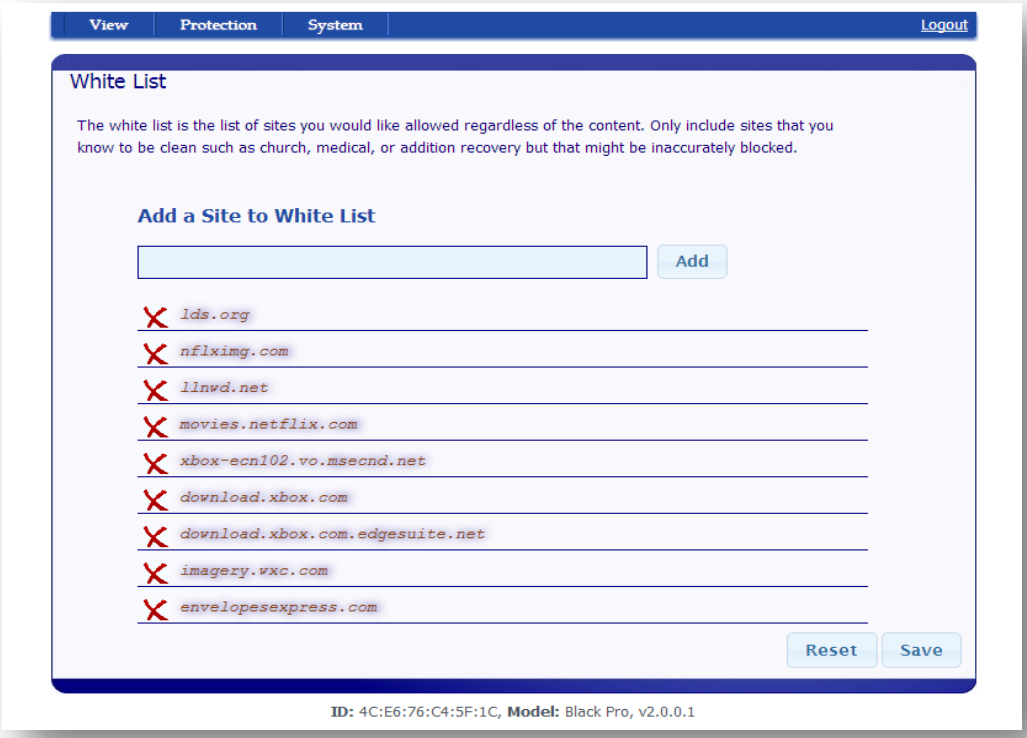
Location: Protection Tab > White list

The white list is a list of websites to be permitted regardless of the content contained on them. This tool is useful for allowing websites that may be incorrectly targeted by the Pandora's Hope filter. To add an entry into the white list:

- Enter in the web address into the blue area .
  (**Note**: You do not need the prefixes HTTP or WWW.)
- Click the "Add" button
- Once all of the desired addresses have been added, click "Save"
- The newly white listed websites will be permitted immediately after pressing "Save"
  Important! Any web address in the white list will be UNFILTERED.

To remove an entry from the Whitelist:

- Press the red "X" next to the web address
- Once all of the desired web addresses have been removed, click "Save"



Chapter 4:

The Filtering Mechanism

4.2c: Configuring the filter: The Grey List

Location: Protection Tab > Grey list

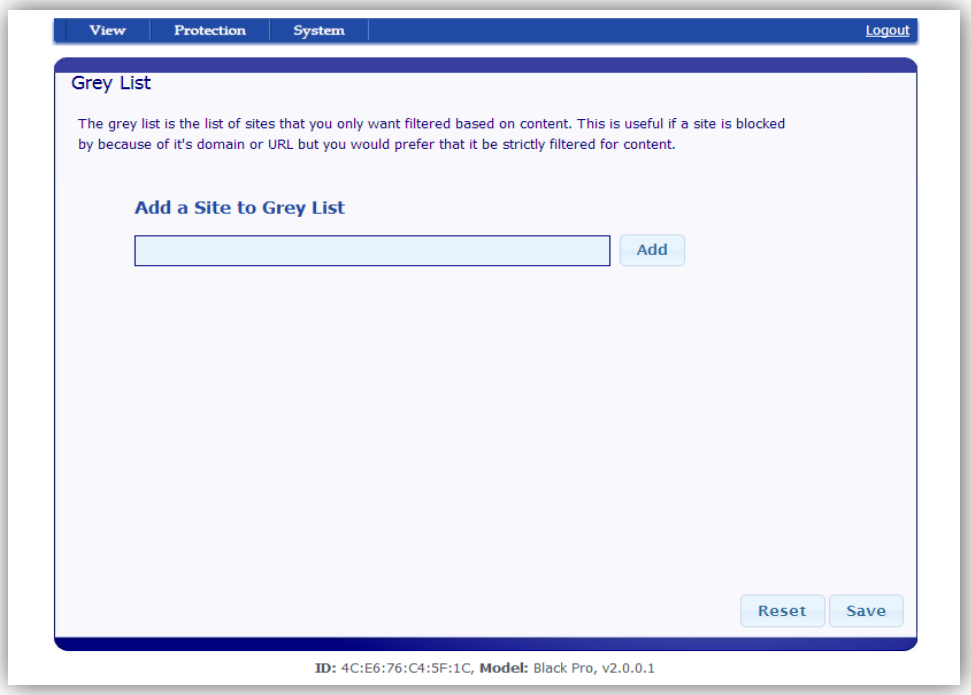
The Grey list is a list of websites to be permitted regardless of their URL. This tool is useful for allowing websites whose addresses may targeted by the Pandora's Hope filter.

To add an entry into the Grey list:

- Enter in the web address into the blue area .
  (**Note**: You do not need the prefixes HTTP: or WWW.)
- Click the "Add" button
- Once all of the desired addresses have been added, click "Save"
- The newly grey listed websites will be permitted immediately after pressing "Save"

To remove an entry from the grey list:

- Press the red "X" next to the web address
- Once all of the desired web addresses have been removed, click "Save"



Chapter 4:

The Filtering Mechanism

4.2d: Configuring the filter: The Keyword List

Location: Protection Tab > Keyword list

The Keyword List is a user defined list of keywords and phrases to be used by the filtering system to block content. Websites containing these keywords and phrases will be blocked, regardless of any other content contained on them. This tool is useful for customizing the type of content Pandora's Hope will block.

To add an entry into the Keyword List:

- Enter in the words or phrases into the area labeled: "Add Keyword or Phrase"
- Hit the enter key when the word or phrase has been typed out.
- The newly added keyword or phrase will then be displayed in a white box.
- Once all of the desired keywords or phrases have been entered, click the "Save" button

To remove an entry from the keyword list:

- Press the blue "X" next the word or phrase
- Once all of the desired keywords or phrases have been removed, click "Save"

Chapter 4:

The Filtering Mechanism

4.2e: Configuring the filter: The Filter Level

Location: Protection Tab > Filter Level

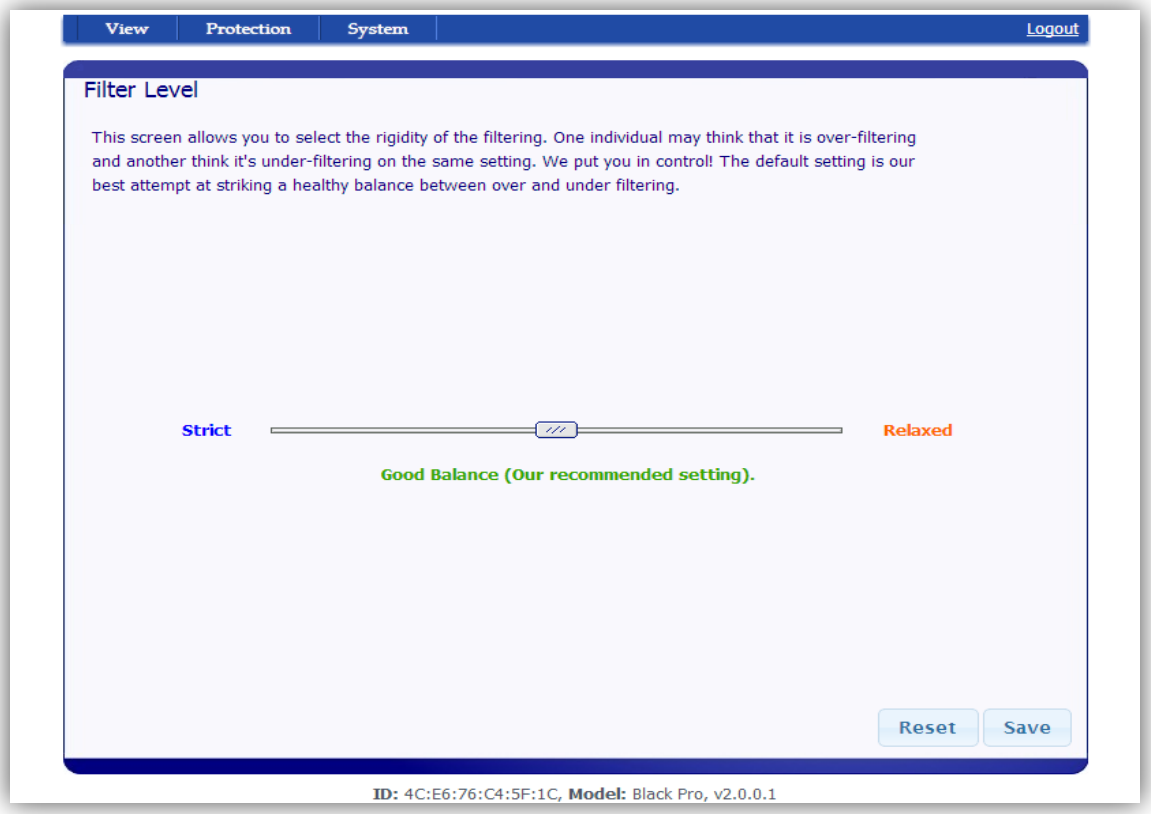
The Filter Level tool allows a user to easily adjust the rigidity of the filter. By default, the filter is set to "Good Balance".

To increase the filter strength:

- Move the slider to the left in small increments, repeating as necessary. As the slider moves more to the left, the user will receive indicator messages.
- Click "Save" once the filter level has been set

To decrease the filter strength:

- Move the slider to the right in small increments, repeating as necessary. As the slider moves more to the right, the user will receive indicator messages.
- Click "Save" once the filter level has been set



Chapter 4:

The Filtering Mechanism

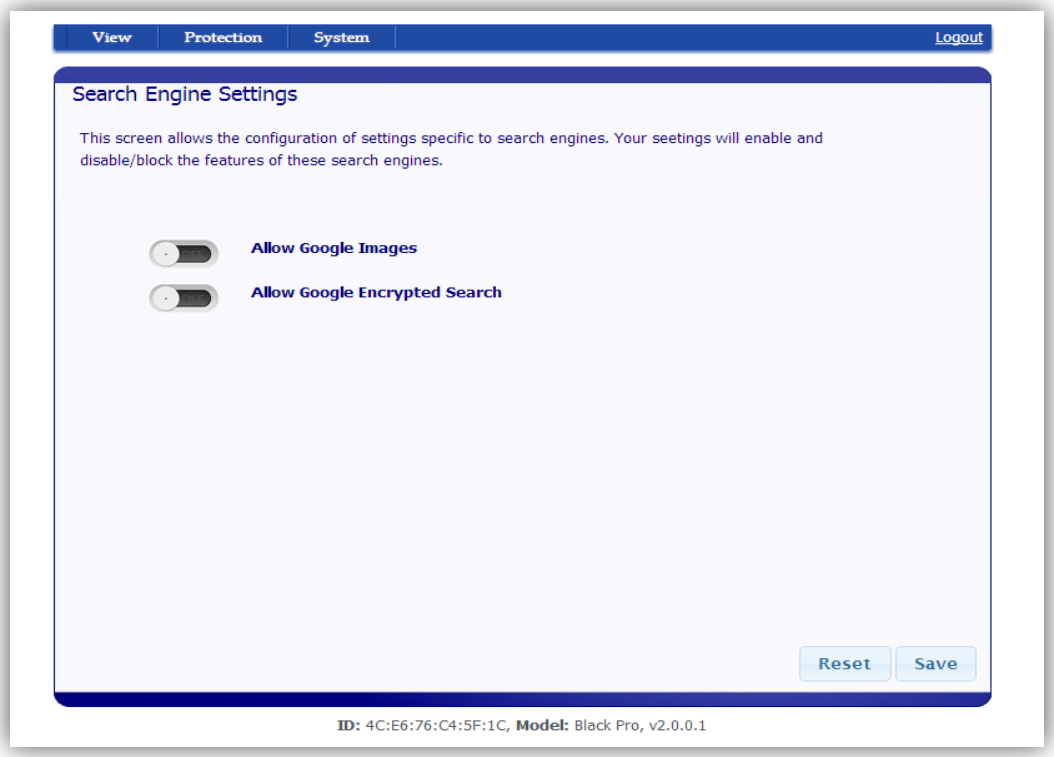
4.2f: Configuring the filter: Search Engine Settings

Location: Protection Tab > Search Engine Settings

The Search Engine Settings page allows the user to customize certain functions related to Google Search.

- **Allow Google Images:**
  This feature will enable or disable the use of Google Images. By default it is set to off.
  To allow the use of Google Images, click on the corresponding button. The switch will turn yellow to indicate that it has been activated. Click the "Save" button once all desired options have been activated.
  Important: Google Images can present a serious internet safety risk, and is best blocked, or used with discretion.

- **Allow Google Encrypted Search:**
  This feature will allow the user to permit the use of encrypted Google searches through: Https://Google.com
  Important: Encrypted searches cannot be filtered, and may return undesired results.



Chapter 4:

The Filtering Mechanism

4.2g: Configuring the filter: Filtering Categories

Location: Protection Tab > Categories

The Categories page allows the user to easily customize the filtering mechanism, based on predefined categories.

To Activate/Deactivate a category :

- Press the corresponding switch.
- Click “Save” when all changes have been made

Chapter 4:

The Filtering Mechanism

4.2h: Configuring the filter: Exclude From Filter

Location: Protection Tab > Exclude from Filter

The Exclude from Filter tool allows the user to disable the filtering system entirely for a specific device. This tool is especially useful for the following devices (Which Pandora's Hope **cannot** filter):

-DVRs (TiVo, Dish Hopper)

-Media players (Roku , Apple TV)

To use the Exclude from Filter tool:

- Enter in the MAC address for the device into the "Add MAC address" field, or use the "This Computer" function (If the device is connected to Pandora's Hope, then the DHCP Clients page will also list the MAC address)
- Click "Add" once the MAC address has been entered
- Press "Save" once all of the desired MAC addresses have been entered
- To **remove** a device from the exclusion list, click on the red "X" next to the MAC address. Then click "Save"

Chapter 4:

The Filtering Mechanism

4.2i: Configuring the filter: Time Restrictions

Location: Protection Tab > Time Restrictions

The Time Restriction function allows the user to specify when a particular device is able to access the internet.

Each Time Restriction rule applies to a single device, and each device can only have a single rule. A Time Restriction rule will activate and deactivate precisely, based on the schedule set. If a user attempts to use the internet during a restricted time, a blocking page will be displayed, informing them of the restriction. This blocking page can be bypassed, using the administrative password. Once bypassed, the user will automatically be directed to the administrative interface, where they can disable the Time Restriction rule.

More information on Time Restrictions can be found on the following page

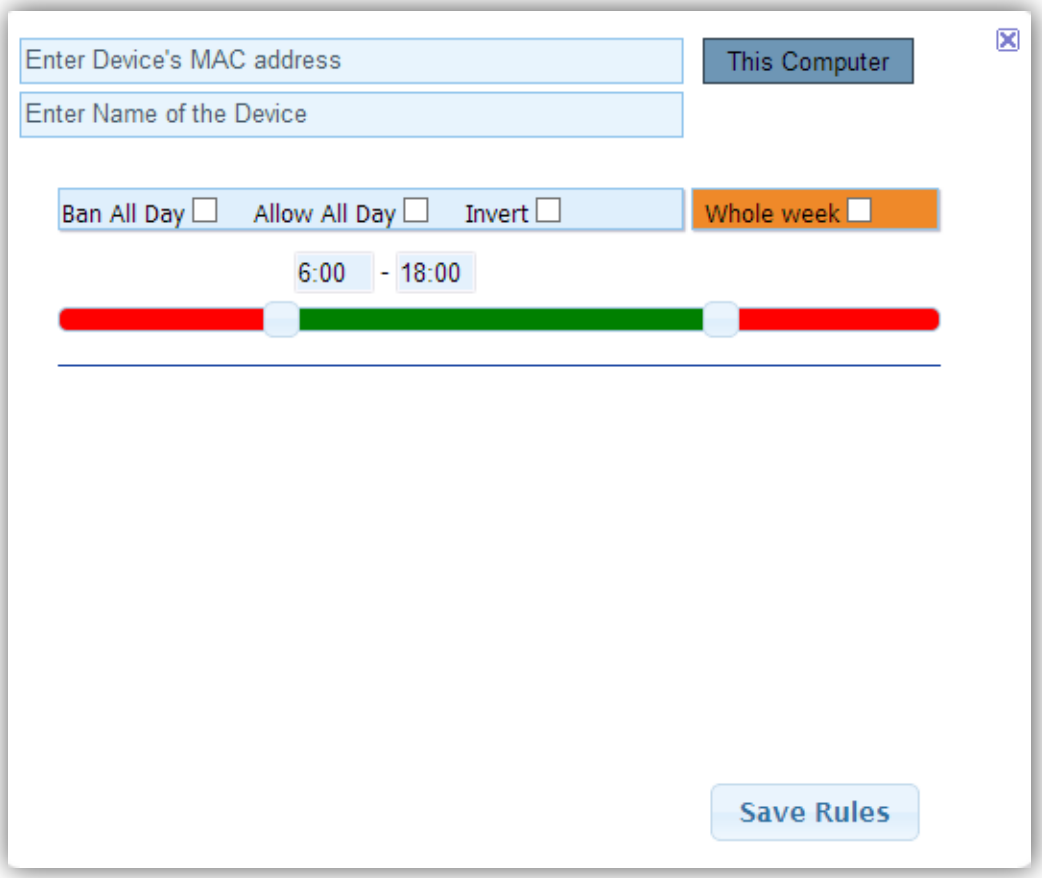
Chapter 4:

The Filtering Mechanism

4.2i: Configuring the filter: Time Restrictions (Continued)

To use the Time restriction function:

- Enter in the MAC address for the device into the "Device's MAC" field, or use the "This Computer" function (If the device is connected to Pandora's Hope, then the DHCP Clients page will also list the MAC address)
- Label the Time Restriction rule by entering a name into the "Enter Name" field
- There are four check boxes that define part of the rule:
  -Ban All Day will restrict the device for the entire day (or days)
  -Allow All Day will permit internet access for the entire day (or days)
  -Invert will reverse the "Allowed" and "Restricted" ranges.
  -Whole week allows each individual day to be customized with a different range.
- Once the desired values have been set, the "Save Rules" button must be pressed to activate the rule
- To edit an existing rule, press the "Pencil" icon next to the rule
- To remove a rule, press the red "X" next to the rule



Chapter 4:

The Filtering Mechanism

4.2j: Configuring the filter: Ad-Driven Websites

Location: Protection Tab > Ad-Driven Sites

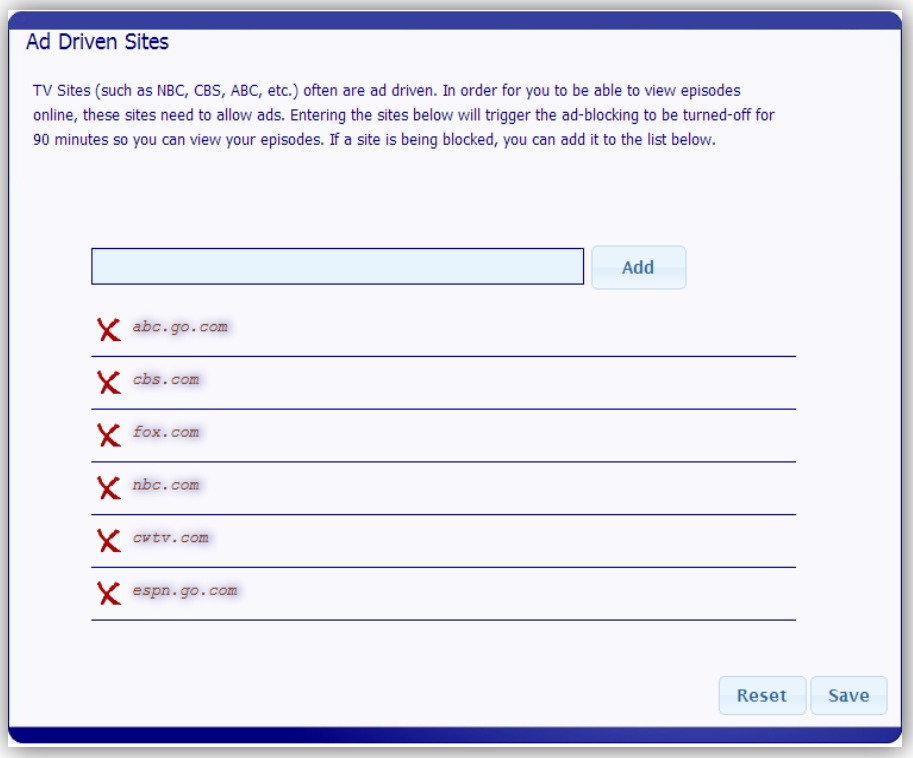
The Ad-Driven Sites tool allows the user to disable the ad-blocking service on Pandora's Hope for a particular webpage. This is useful for viewing websites that require advertisements to function.

To add an entry into the Ad-Driven sites tool:

- Enter in the web address into the blue area .
  (**Note**: You do not need the prefixes HTTP: or WWW.)
- Click the "Add" button
- Once all of the desired addresses have been added, click "Save"
- The newly added websites will be permitted to display advertisements immediately after pressing "Save"

To remove an entry from the Ad-Driven Sites tool:

- Press the red "X" next to the web address
- Once all of the desired web addresses have been removed, click "Save"



Chapter 4:

The Filtering Mechanism

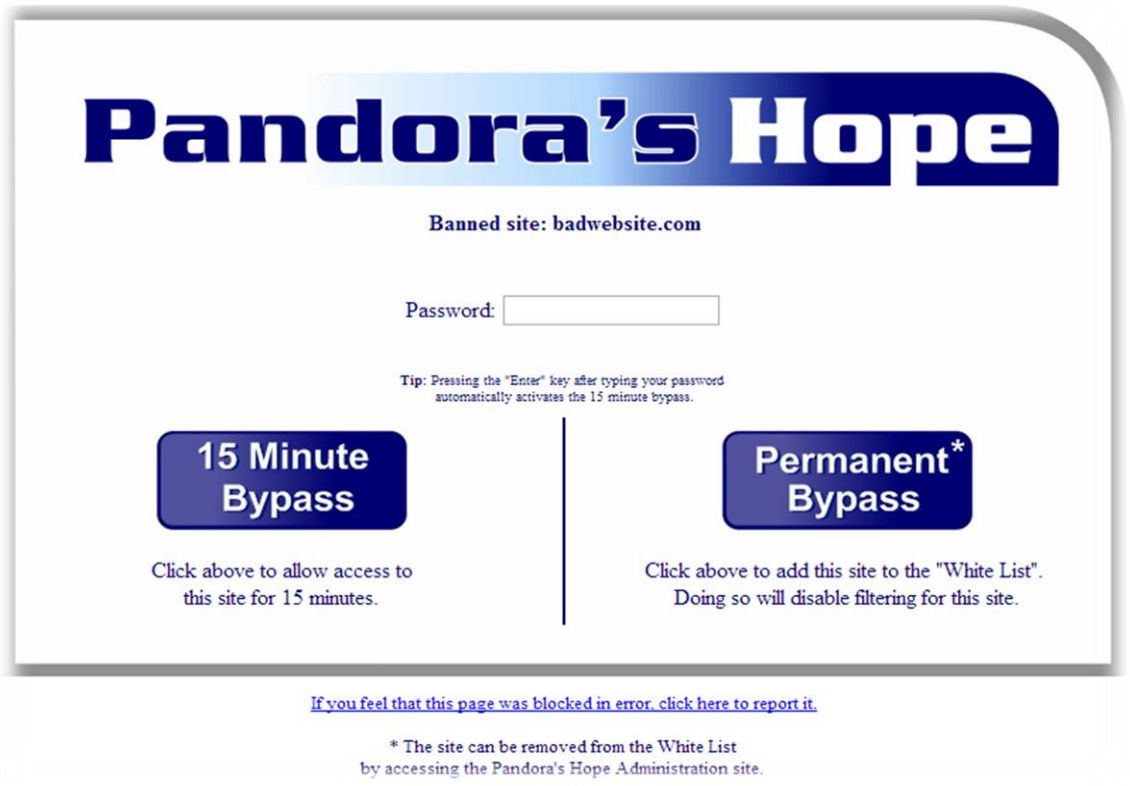
4.3: The Blocking Page

The “Blocking Page” is the webpage displayed when inappropriate content has been detected. This page allows the user to bypass a block, either temporarily (15 minutes), or permanently (The website is white listed).

To authorize a bypass:

- Enter the administrative password into the “Password” field
- Select the Temporary, or Permanent options.
  (The Temporary option is usually the safest)

Important: Using the Bypass option will leave the destination website **unfiltered**



Chapter 5:

System Settings

5.1: Wireless Configuration

Location: System > Wireless Configuration

The Wireless Configuration page allows the user to change various aspects of the wireless network. Descriptions of the options found on this page are located below.

Important! The settings on this page have the ability to bring down the wireless network. Use with caution.

Option Descriptions:

-*Enable Wireless access:* This will Activate or Deactivate the wireless network

-*Channel:* This will change the wireless channel. By default this value is set to" 5"

-*Broadcast SSID:* This will show or hide the wireless network name (SSID)

-*SSID:* This is the name of the wireless network

-*Enable Wireless Security:* This enables or disables wireless network security

-*Security Type:* Changes the wireless security standard. By default this is set to "WPA2"

-*Key:* This is the wireless network security key, used to connect wireless devices to Pandora's Hope

-*Enable MAC Filtering:* This enables the MAC filtering option, which can be used to prevent devices with specific MAC addresses from connecting to the wireless network.

-*Protocol:* This sets the IEEE wireless standard to be used. By default this is set to "11ng."

-*Channel Width:* This changes the width of the wireless channel. By default this is set to "40MHz Upper"

-*No Scan:* This option enables or disable the auto-scanning functionality of the router. By default it is set to "On"

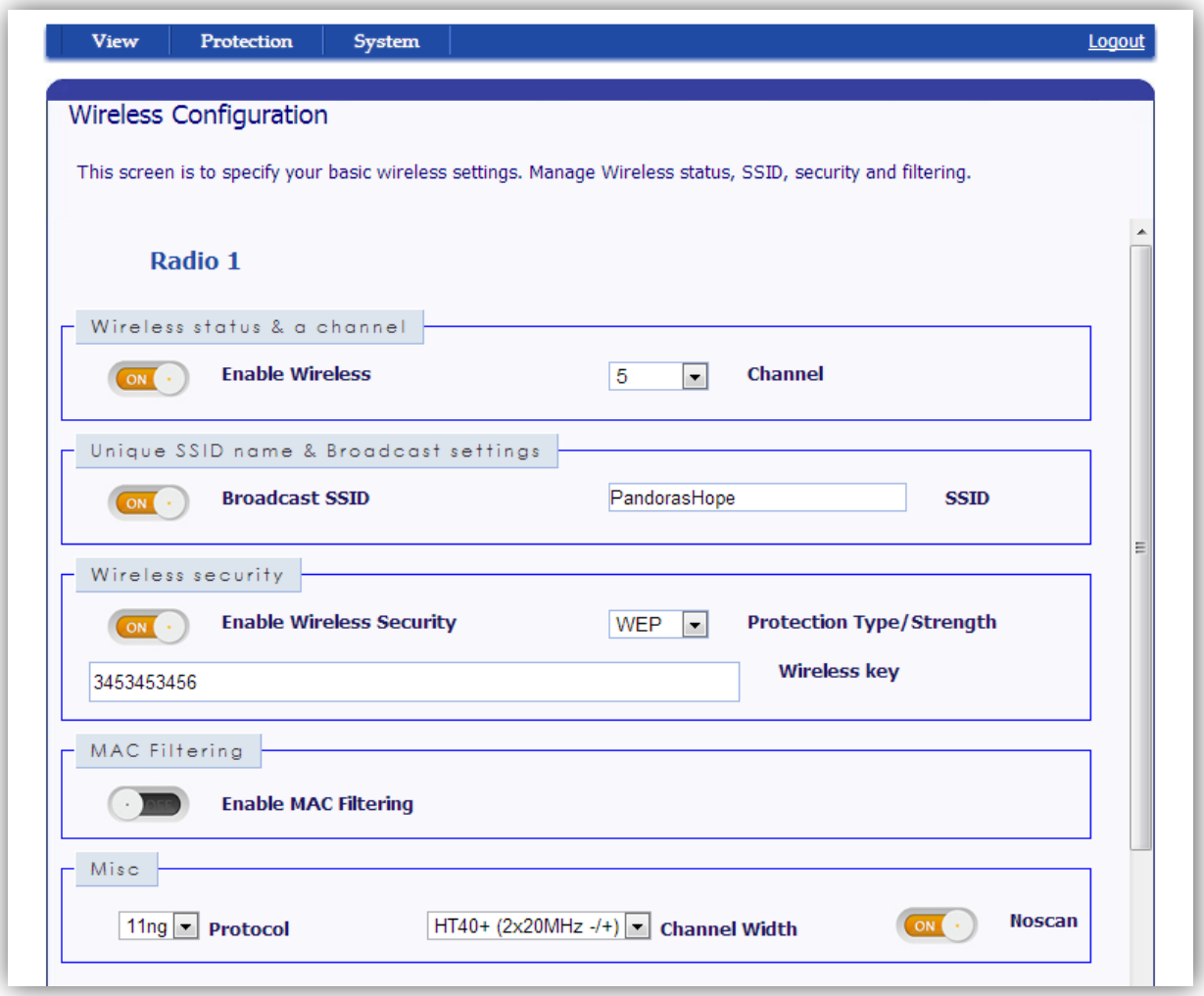
Pro version users: There will be a second radio, which will also have the settings above. This is for the 5Ghz radio.

Chapter 5:

System Settings

5.1a: Wireless Configuration (Continued)

This is the wireless configuration page



Chapter 5:

System Settings

5.2a: Network Configuration: General Settings

Location: System > General

The General page contains settings that allow the user to change the IP addressing of the WAN, and LAN interfaces.

Important! The settings on this page have the ability to render Pandora's Hope inoperable. Use with caution.

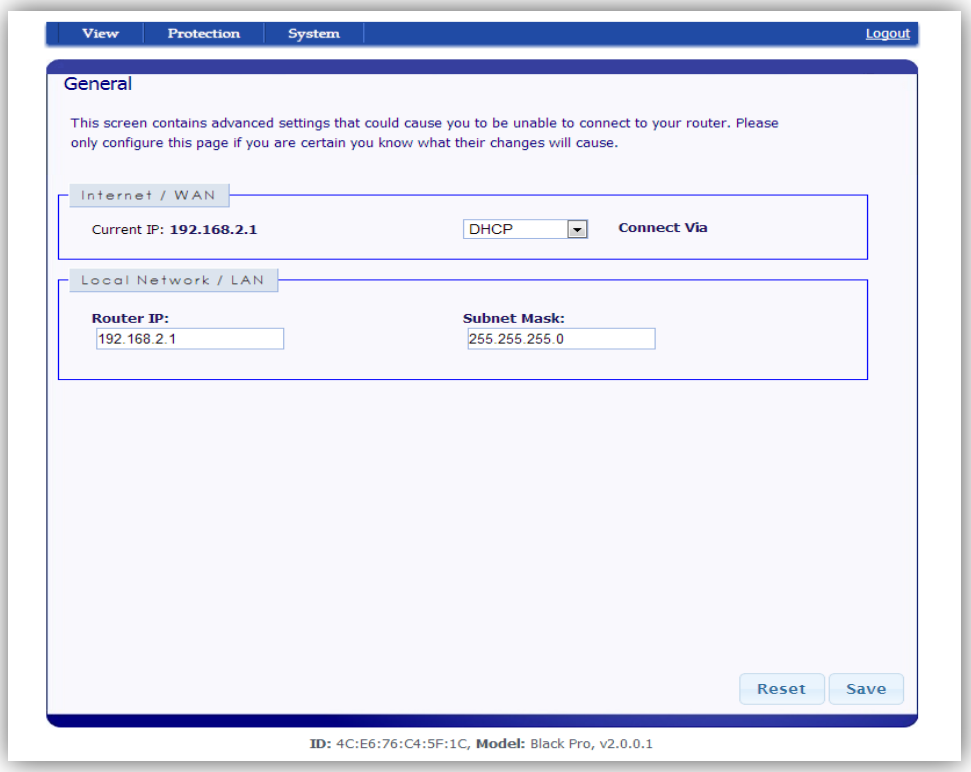
Internet/WAN Settings

-The "Connect Via" drop-down menu allows the user to set the WAN interface to a static address. This is usually reserved for special circumstances, where an ISP's equipment requires the use of a static IP address. When switching to a static address, the user will need to populate the new settings with information provided from their ISP.

Local Network / LAN Settings

-The "Router IP" field allows the user to change the IP addressing scheme for Pandora's Hope. By default, Pandora's Hope uses the **192.168.2.1** network.

-The "Subnet Mask" field allows the user to set the appropriate subnet mask information.



Chapter 5:

System Settings

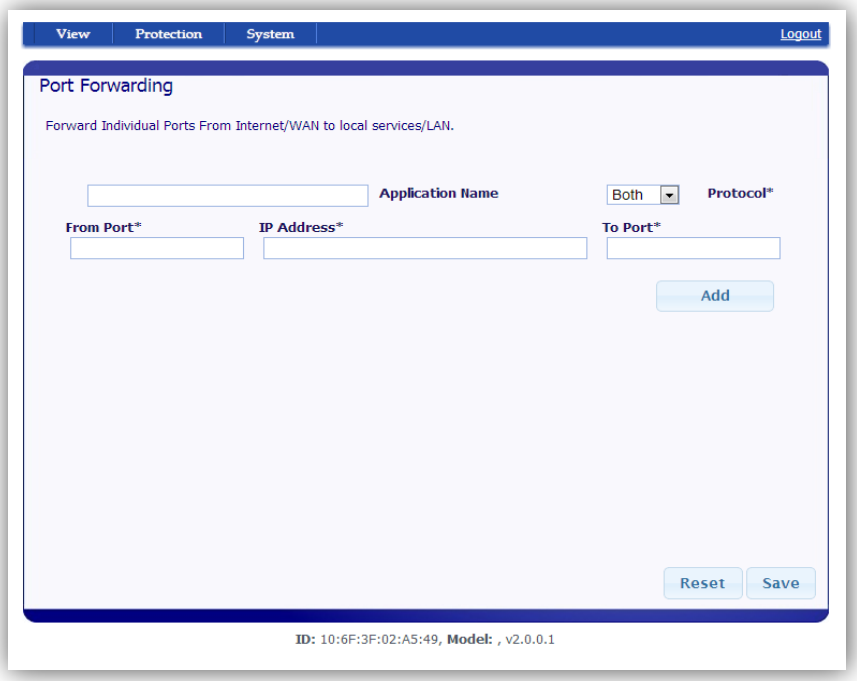
5.2b: Network Configuration: Port Forwarding

Location: System > Port Forwarding

The Port Forwarding tool allows the user to permit and redirect incomming information through specifc ports, for a particular device. This tool is useful in getting some applications and devices working through Pandora's Hope, which may requrie a specifc port to be open.

To create a port forwarding rule:

- Enter in a name for the new rule in the "Application Name" field.
- Enter in the "From port" number. This will be the original port number
- Enter in the IP address for the device you would like the rule to govern.
- Enter in the "To port" number. This number is set by the user.
  -If the "To" and "From" ports are identical, traffic across that port will not be redirected, but permitted
  -If the "To" and "From" ports differ, traffic coming through the "From" port will be redirected to the "To" port
- Select the Protocol to be used by the port forwarding rule.
- To create the new port forwarding rule, press the "Add" button
- Once all of the desired rules have been added, press "Save"



Chapter 5:

System Settings

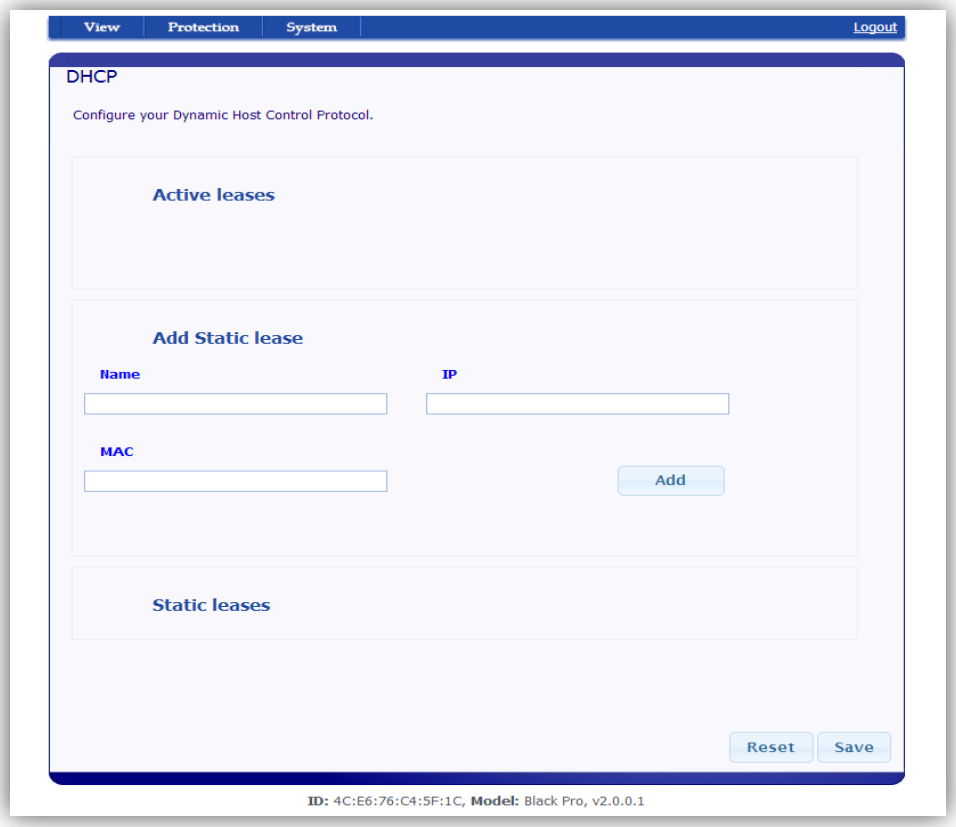
5.2c: Network Configuration: DHCP Settings

Location: System > DHCP Settings

The DHCP Settings page allows the user to create static leases for their devices. A static lease prevents the IP address of a computer from changing.

To create a static lease:

- Enter in a name in the "Name" field. This name is superficial, and can be whatever the user prefers.
- Enter in the desired IP address for the device in the "IP" field
- Enter in the MAC address for the device in the "MAC" field (See page **3.4** for more information)
- Once all of the required information has been entered, press Add.
- Once all of the desired static leases have been entered, press Save



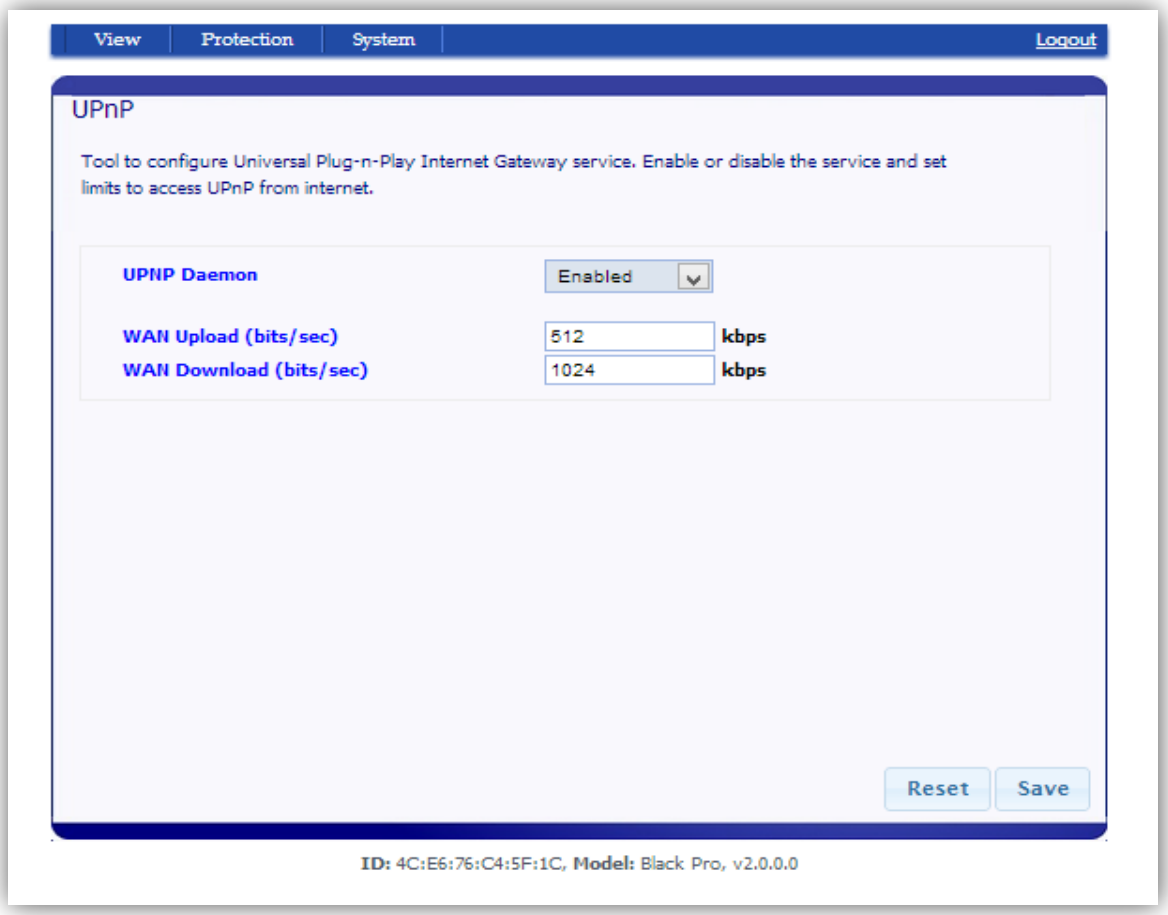
Chapter 5:

System Settings

5.2d: Network Configuration: UPnP

Location: System > UPnP

The Universal Plug-n-Play tool allows the user to modify UPnP settings. UPnP is a set of network protocols, that allows networked devices to automatically discover each other. These settings should remain unchanged, unless the user has a specific reason to modify them.



Chapter 5:

System Settings

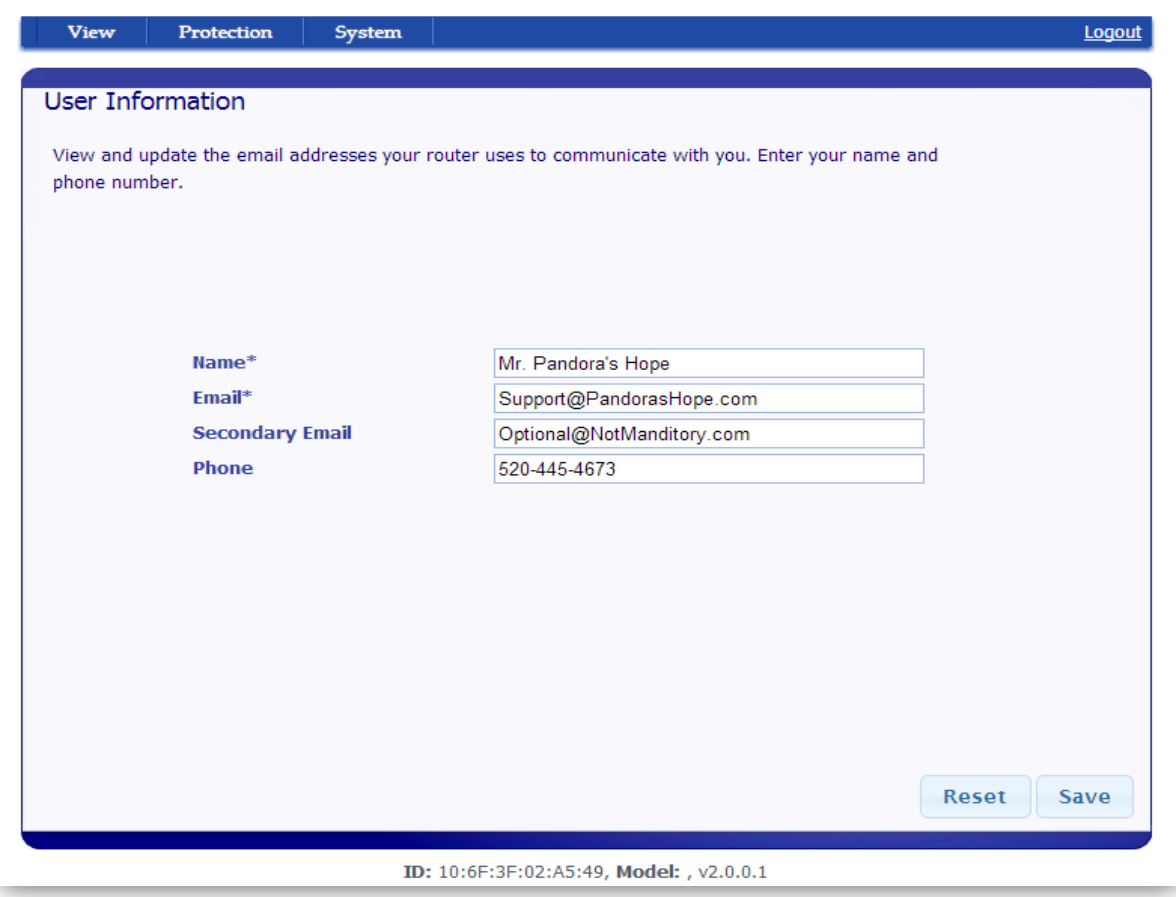
5.3: User Information

Location: System > User Information

The User Information page displays the personal information of the account holder. This information can be modified at any time through this page.

To update the user's information:

- Make the necessary changes.
- When all changes have been made, press Save



Chapter 5:

System Settings

5.4: Resetting the Administrative Password

Location: System > Password

The Password tool allows the user to change the administrative password.

To create a new password:

- Enter in the desired password in the “Password” field.
- Confirm this password in the “Confirm Password” field.
- Once the new password has been entered in twice, press Save

Important! If the administrative password has been lost, the user will need to contact the Pandora’s Hope support team:

1-520-445-4673

Support@PandorasHope.com